UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,227	04/05/2001	Philip D. MacKenzie	9	6212

7590 09/20/2005		EXAMINER
Ryan, Mason & Lewis, LLP		MOORTHY, ARAVIND K
90 Forest Avenue		

ART UNIT	PAPER NUMBER
2131	

Locust Valley, NY 11560

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/827,227	MACKENZIE, PHILIP D.
	Examiner	Art Unit
	Aravind K. Moorthy	2131

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE **3** MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 September 2005*.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1,3-8,10,12-17,19 and 20* is/are rejected.
7)☒ Claim(s) *2,9,11 and 18* is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on *09 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
        1.☐ Certified copies of the priority documents have been received.
        2.☐ Certified copies of the priority documents have been received in Application No. _____.
        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 2 September 2005.

2. Claims 1-20 are pending in the application.

3. Claims 1, 3-8, 10, 12-17, 19 and 20 have been rejected.

4. Claims 2, 9, 11 and 18 have been objected to.

Response to Arguments

5. The indicated allowability of claims 1, 3-8, 10, 12-17, 19 and 20 is withdrawn in view of the

newly discovered reference(s) to Wu. Rejections based on the newly cited reference(s) follow.

Terminal Disclaimer

6. The terminal disclaimer filed on 6 June 2005 disclaiming the terminal portion of any patent

granted on this application which would extend beyond the expiration date of any patent granted

on Application number 09/638,320 has been reviewed and is accepted. The terminal disclaimer

has been recorded.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 3-8, 10, 12-17, 19, and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Wu U.S. Patent No. 6,539,479 B1.

As per claims 1, 10, and 19, Wu teaches a method for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, said group having a group operation and an inverse group operation, said method comprising the steps of [column 5 line 28 to column 6 line 9]: one party generating a parameter m by performing the group operation on g^x and a function of at least said password, wherein any portion of a result associated with the function that is outside the group is randomized and transmitting m to the other party, whereby the other party may perform the inverse group operation on m and said function of at least said password and remove the randomization of any portion of the result associated with the function that is outside the group, to extract g^x and further calculate said shared secret g^{xy} [column 5 line 28 to column 6 line 9].

As per claims 8, 17, and 20, Wu teaches a method for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy}, where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, said group having a group operation and an inverse group operation, said method comprising the steps of [column 5 line 28 to column 6 line 9]: responsive to one party generating a parameter m by performing the group operation on g^x and a function of at least said password, wherein any portion of a result associated with the function that is outside the group is randomized and

transmitting m to the other party, whereby the other party may perform the inverse group operation on m and said function of at least said password and remove the randomization of any portion of the result associated with the function that is outside the group, to extract g^x and further calculate said shared secret g^{xy} [column 5 line 28 to column 6 line 9].

As per claims 3 and 12, Wu teaches one party is a client and said other party is a server [column 6, lines 10-13].

As per claims 4 and 13, Wu teaches said one party receiving g^y from said other party and generating said shared secret g^{xy} [column 5 line 63 to column 6 line 15].

As per claims 5 and 14, Wu teaches one party authenticating said other party by comparing a received value against a function of at least one of an identifier of said one party, an identifier of said other party, m, g^y, the shared secret, and the password (verifier) [column 5 line 28 to column 6 line 9 and column 7, lines 45-59].

As per claims 6 and 15 Wu teaches said one party transmitting a function of at least one of an identifier of said one party, an identifier of said other party m, g^y, the shared secret, and the password (verifier), to said other party whereby the other party may authenticate said one party [column 5 line 28 to column 6 line 9].

As per claims 7 and 16 Wu teaches one party generating a session key as a function of a least one of an identifier of said one party, an identifier of said other party, m, g^y, the shared secret, and the password [column 5 line 28 to column 6 line 9].

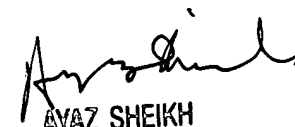## *Conclusion*

8.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
September 13, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100